

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings of claims in the application:

**Listing of Claims:**

1.-8. (Canceled)

9. (Currently amended) A computer-implemented method for ensuring non-repudiation of a payment request obtained from a first organization by a second organization, the method comprising:

storing, in a storage device associated with one or more computer systems associated with the second organization, authority information of users of the first organization independently of authority information incorporated within digital certificates assigned to the users;

receiving, from one or more computer systems associated with the first organization at one or more computer systems ~~operated by an~~ associated with the second organization, a payment request identifying ~~at least~~ at least one payee;

receiving, from one or more computer systems associated with the first organization at the one or more computer systems ~~operated by an~~ associated with the second organization, a digital certificate associated with a user of the first organization that originated the payment request, the digital certificate including a first portion configured to enable authentication of the user by the second organization and a second portion configured to explicitly define authority of the user to request payments, the second portion including a maximum payment amount that the user is authorized to request and a plurality of specific payees to whom the user can request payment certificate identifying information, user-identifying information identifying a user having caused the payment request to be generated, and authority information defining:

——— an authority of the user identified in the user-identifying information to make payment requests;

23                   — a maximum payment that the user identified in the user-identifying  
24 information is authorized to make, and

25                   — a list of specific payees to whom the user identified in the user-identifying  
26 information is authorized to make payments;

27                   retrieving, with one or more processors associated with the one or more computer  
28 systems ~~operated by an~~ associated with the second organization, stored authority information  
29 associated with the user of the first organization identified in the user-identifying information  
30 from a store of authority information hosted outside the first organization by the second  
31 organization and that is independent of the received digital certificate;

32                   validating, with the one or more processors associated with the one or more  
33 computer systems ~~operated by an~~ associated with the second organization, the authority  
34 ~~information of the user explicitly defined~~ within the received digital certificate based on a  
35 comparison between the retrieved stored authority information and ~~the authority~~ information  
36 included within the received digital certificate representing the maximum payment amount that  
37 the user is authorized to request and the plurality of specific payees to whom the user can request  
38 payment; and

39                   generating ~~information~~, with the one or more processors associated with the one  
40 or more computer systems ~~operated by an~~ associated with the second organization, information  
41 authorizing the payment request in response to a validation of the authority ~~information included~~  
42 of the user explicitly defined within the received digital certificate ~~when the at least one payee~~  
43 ~~identified in the payment request is included in the list of specific payee defined in the authority~~  
44 ~~information included within the received certificate.~~

1                   10. (Currently amended) The method of claim 9, wherein ~~the payment request~~  
2 ~~is for a predetermined amount and wherein authorizing the payment request further generating~~  
3 the information authorizing the payment request in response to a validation of the authority of  
4 the user explicitly defined within the received digital certificate comprises authorizing the  
5 payment request when the maximum payment amount that the user ~~identified in the user-~~

identifying information is authorized to ~~make request~~ is at least greater than or equal to ~~[[the]]~~ a predetermined amount associated with the payment request.

11. (Currently amended) The method of claim 9, wherein the received digital certificate conforms to the X.509 standard.

12. (Currently amended) The method of claim 9, wherein the authority ~~information included in~~ of the user explicitly defined within the received digital certificate is configured as XML code.

13. (Original) The method of claim 9, wherein the XML code is compliant with a DSML standard.

14. (Canceled)

15. (Currently amended) A non-transitory computer-readable ~~storage~~ medium storing computer-executable code for ensuring non-repudiation of a payment request obtained from a first organization by a second organization carrying out a financial transaction, the ~~non-transitory~~ computer-readable ~~storage~~ medium comprising:

code for receiving a payment request from a first organization by a second organization, the payment request identifying at least at least one payee;

code for receiving a digital certificate associated with a user of the first organization that originated the payment request, the digital certificate including a first portion configured to enable authentication of the user by the second organization and a second portion configured to explicitly define authority of the user to request payments, the second portion including a maximum payment amount that the user is authorized to request and a plurality of specific payees to whom the user can request payment certificate-identifying information;

code for retrieving stored authority information associated with the user of the first organization from a store of authority information hosted outside the first organization by the second organization and that is independent of the received digital certificate;

code for validating the authority of the user explicitly defined within the received digital certificate based on a comparison between the retrieved stored authority information and information included within the received digital certificate representing the maximum payment amount that the user is authorized to request and the plurality of specific payees to whom the user can request payment; and

code for generating information authorizing the payment request in response to a validation of the authority of the user explicitly defined within the received digital certificate.

certificate-receiving code configured to receive a digital certificate including certificate-identifying information, user-identifying information identifying a user responsible for the financial transaction, and authority information defining:

—— an authority of the user to request that the financial transaction be carried out;

—— a maximum transaction amount that the user identified in the user-identifying information is authorized to make, and

—— a list of specific parties with whom the user identified in the user-identifying information is authorized to carry out transactions;

authorization validating code configured to retrieve stored authority information associated with the user identified in the user-identifying information from a store of authority information stored apart from the payment request and that is independent of the received digital certificate and validate the authority information within the received digital certificate based on a comparison between the retrieved authority information and the authority information included within the received digital certificate; and

code for generating information authorizing the financial transaction in response to a validation of the authority information included within the received digital certificate when at least one party to the transaction is included in the list of specific parties defined in the authority information included within the received digital certificate.

16. (Currently amended) The non-transitory computer-readable storage medium of claim 15, wherein the received digital certificate conforms to the X.509 standard.

1                   17.     (Currently amended) The non-transitory computer-readable storage  
2 medium of claim 15, wherein the authority ~~information included in~~ of the user explicitly defined  
3 within the received digital certificate is configured as XML code.

1                   18.     (Currently amended) The non-transitory computer-readable storage  
2 medium of claim 17, wherein the XML code is compliant with a DSML standard.

1                   19.     (Currently amended) The non-transitory computer-readable storage  
2 medium of claim 15, wherein the code for generating the information authorizing the payment  
3 request in response to a validation of the authority of the user explicitly defined within the  
4 received digital certificate comprises code for authorizing the payment request when the  
5 maximum payment amount that the user is authorized to request is at least greater than or equal  
6 to a predetermined amount associated with the payment request authority defined in the authority  
7 information within the received digital certificate also defines rights of the user to access  
8 predetermined data and programs associated with the financial transaction.

20.-28. (Canceled)

1                   29.     (Currently amended) A system for ensuring non-repudiation of a payment  
2 request server computer to authenticate a user of a client computer and to verify that the user is  
3 authorized to request that the server computer carry out a requested action, the system server  
4 computer comprising:

5                   a storage device configured to store authorization information associated with  
6 users of an organization independently of authority information incorporated within digital  
7 certificates assigned to the users;

8                   a processor; and  
9                   a memory coupled to the processor and configured to store a set of instructions  
10 that when executed by the processor causes the processor to:

11                   receive a payment request identifying at least at least one payee;

12 receive a digital certificate associated with a user of the organization that  
13 originated the payment request, the digital certificate including a first portion configured  
14 to enable authentication of the user by another organization and a second portion  
15 configured to explicitly define authority of the user to request payments, the second  
16 portion including a maximum payment amount that the user is authorized to request and a  
17 plurality of specific payees to whom the user can request payment;

18 retrieve stored authority information associated with the user of the first  
19 organization identified in the user-identifying information from the storage device, the  
20 retrieved stored authority information being independent of the received digital  
21 certificate;

22 validate the authority of the user explicitly defined within the received  
23 digital certificate based on a comparison between the retrieved stored authority  
24 information and information included within the received digital certificate representing  
25 the maximum payment amount that the user is authorized to request and the plurality of  
26 specific payees to whom the user can request payment; and

27 generate information authorizing the payment request in response to a  
28 validation of the authority of the user explicitly defined within the received digital  
29 certificate.

30 ——— receive a payment request along with a digital certificate assigned to the  
31 user of the client computer, the digital certificate comprising a first code portion and a second  
32 code portion;

33 ————— wherein the first code portion of the digital certificate is configured  
34 to enable authentication of the user, the first code portion defining a public key, a certificate  
35 serial number, a certificate validity period, a digital signature of the certificate authority, and an  
36 extension field;

37 ————— wherein the second code portion of the digital certificate is  
38 configured to define an authority of the user of the client computer to request that the server  
39 computer carry out the requested action, the second code portion being configured for inclusion  
40 within the extension field of the first code portion, the authority of the user defined within the

second code portion of the certificate defining access rights of the user including a maximum payment that the user is authorized to make and a list of specific payees to whom the user is authorized to make payments;  
—— retrieve, from a store of authority information, stored authority information associated with the user of the client computer that is stored apart from the payment request and that is independent of the received digital certificate;  
—— validate the authority information within the digital certificate based on a comparison between the retrieved authority information and the authority information included within the digital certificate; and  
—— generate information authorizing the payment request in response to a validation of the authority information within the digital certificate when the at least one payee identified in the payment request is included in the list of specific payee defined in the authority information included within the received certificate.

30. (Currently amended) The ~~server computer~~ system of claim 29, wherein the digital certificate conforms to the X.509 standard.

31. (Currently amended) The ~~server computer~~ system of claim 29, wherein the ~~second code portion~~ authority of the user explicitly defined within the received digital certificate is configured as XML code.

32. (Currently amended) The ~~server computer~~ system of claim 31, wherein the XML code is compliant with a DSML standard.

33. (Currently amended) The ~~server computer~~ system of claim 29, wherein the processor is caused to authorize the payment request when the maximum payment amount that the user is authorized to request is at least greater than or equal to a predetermined amount associated with the payment request to generate the information authorizing the payment request in response to a validation of the authority of the user explicitly defined within the received

- 6 digital certificate the authority of the user of the client computer is stored in a hierarchical
- 7 ~~authority data structure that is accessible by the server computer.~~